
The Parliament of the Commonwealth of Australia

Review of the Cybercrime Legislation Amendment Bill 2011

Joint Select Committee on Cyber-Safety

August 2011
Canberra

© Commonwealth of Australia 2011

ISBN 978-0-642-79554-0 (Printed version)

ISBN 978-0-642-79555-7 (HTML version)



Contents

Membership of the Committee	vii
Terms of reference	ix
List of abbreviations	x
List of recommendations	xi
1 Introduction	
Conduct of the inquiry	1
Previous parliamentary consideration	2
2 Outline of the European Convention on Cybercrime and the Cybercrime Bill	
Introduction	5
European Convention on Cybercrime	5
Cybercrime Legislation Amendment Bill 2011	7
Telecommunications Act 1997	8
Telecommunications (Interception and Access) Act 1979	9
Mutual Assistance in Criminal Matters Act 1987	9
Criminal Code Act 1995	10
3 Domestic and Foreign Preservation Notices	
Introduction	11
European Convention on Cybercrime	11
Cybercrime Legislation Amendment Bill 2011	12

Domestic preservation notices	12
Period in force	13
Enforcement agencies and interception agencies	13
Thresholds - enforcement agencies	14
Thresholds - ASIO	14
Revocation	15
Foreign preservation notices	15
Threshold	16
Revocation	16
Commentary	17
Distinction between content and traffic data	17
Distinction between ongoing preservation and interception	19
Threshold – serious offence and serious contravention	20
Foreign countries	21
Committee View	21
4 Mutual Assistance - Stored Communications and Disclosure of Prospective Data to Foreign Countries	
Introduction	23
European Convention on Cybercrime	23
Cybercrime Legislation Amendment Bill 2011	24
Stored Communications Warrants	24
Thresholds	25
Safeguards	25
Conditions of Disclosure	26
Commentary	26
Conditions of disclosure	30
Mutual assistance regime	30
Committee View	31
Disclosure of Prospective Telecommunications Data	33
Threshold	33
Safeguard	33
Conditions of disclosure	34
General Privacy Safeguard	34

Commentary	34
Committee View	36
5 Police Assistance to Foreign Countries – Historic and Existing Telecommunications Data	
Introduction	37
Background	37
Cybercrime Legislation Amendment Bill 2011	38
Primary disclosure of historical telecommunications data	38
Secondary disclosure of existing telecommunications data	39
Privacy safeguard	40
Restriction on use, disclosure, retention and destruction of telecommunications data.....	40
Commentary	40
Thresholds	40
Dual criminality.....	42
Privacy safeguard	42
Conditions of disclosure	43
Notification to data subjects	44
Committee View	45
Threshold	45
6 Commonwealth Computer Offences	
Introduction	49
Cybercrime Legislation Amendment Bill 2011	50
Impact on the validity of concurrent State criminal offences.....	51
Direct versus indirect inconsistency	53
Committee View	54
7 Reporting and Oversight	
Introduction	57
Cybercrime Legislation Amendment Bill	57
Commentary	58
Effective and purposeful oversight	58
Inspection of carrier’s access, storage and disclosure of communications	60

Disclosures to foreign countries	61
Committee View	62
8 Industry Data Handling and Privacy Obligations	
Introduction	65
Existing obligations to assist law enforcement	65
Commentary	66
Context of European law	69
Committee View	70
9 Industry Implementation Issues	
Introduction	73
Implementation Issues	73
Transitional period.....	73
European standards.....	74
Cost recovery.....	75
Telstra recommendations.....	76
Attorney-General's Department response	76
Committee View	77
Additional Comments—Senator Scott Ludlam, Australian Greens.....	79
Appendix A — Submissions	83
Appendix B — Witnesses	85
Appendix C – Enforcement Agencies	87
Agencies that can authorise the disclosure of existing non-content information	88
Agencies that can authorise the disclosure of non-content information on a prospective basis.....	88
Appendix D – Interception Agencies.....	91
Appendix E – Framework for Access to Communications in Australia.....	93

Committee Secretariat

Secretary	Mr James Catchpole
Inquiry Secretary	Ms Jane Hearn
Administrative Officers	Ms Heidi Lushtinetz
	Ms Michaela Whyte



Terms of reference

On 23 June 2011, the House of Representatives adopted the report by the House of Representatives Selection Committee entitled *Report No. 26: Consideration of Bills*.

In that report, the Selection Committee determined that the Cybercrime Legislation Amendment Bill 2011 be referred to the Joint Select Committee on Cyber-Safety.



List of abbreviations

AFP	Australian Federal Police
ALRC	Australian Law Reform Commission
ASIO	Australian Security Intelligence Organisation
MA Act	<i>Mutual Assistance in Criminal Matters Act 1987</i>
TIA Act	<i>Telecommunications (Interception and Access) Act 1979</i>



List of recommendations

4 Mutual Assistance - Stored Communications and Disclosure of Prospective Data to Foreign Countries

Recommendation 1

That the thresholds that apply to the issuing of a stored communication warrant under the *Mutual Assistance in Criminal Matters Act 1987* and the *Telecommunications (Interception and Access) Act 1979* for an investigation or investigative proceeding for a serious foreign offence be the same thresholds as apply for domestic Australian investigations.

Recommendation 2

That the Attorney-General investigate whether the proposed new Part IIIA of the *Mutual Assistance in Criminal Matters Act 1987* may prevent stored communications warrants being available to foreign countries for investigations into child sexual exploitation.

Recommendation 3

That subsection 8(2) of the *Mutual Assistance in Criminal Matters Act 1987* be amended to include an additional discretionary ground to decline a request where the requesting country's arrangements for handling personal information do not offer privacy protection substantially similar to those applying in Australia.

Recommendation 4

That proposed section 180F of the *Telecommunications (Interception and Access) Act 1979* is amended to elaborate more precisely the requirement that the authorising officer consider and weigh the proportionality of the intrusion into privacy against the value of the potential evidence and needs of the investigation.

5 Police Assistance to Foreign Countries – Historic and Existing Telecommunications Data**Recommendation 5**

That proposed sections 180A (5) and 180C (2) of the *Telecommunications (Interception and Access) Act 1979* be amended to ensure that, in determining whether a disclosure of telecommunications data to a foreign country is appropriate in all the circumstances, the authorising officer must give consideration to the mandatory and discretionary grounds for refusing a mutual assistance request under existing section 8 of the *Mutual Assistance in Criminal Matters Act 1987*.

Recommendation 6

That the disclosure of telecommunications data to a foreign country in the context of police to police assistance at the investigative stage and in relation to criminal conduct that, if prosecuted, may attract the death penalty, must:

- (a) only take place in exceptional circumstances and with the consent of the Attorney-General and the Minister for Home Affairs and Justice; and
- (b) each Minister must ensure that such consent is recorded in a register for that purpose.

Recommendation 7

That the Cybercrime Legislation Amendment Bill 2011 be amended to elaborate the conditions of disclosure of historical and existing telecommunications data to foreign countries, including in relation to retention and destruction of the information and an express prohibition on any secondary use by the foreign country.

Recommendation 8

That the Attorney-General investigate the desirability and practicality of a legislative requirement for data subjects to be advised that their communications have been subject to an intercept, stored communications warrant, or telecommunications data disclosure under the *Telecommunications (Interception and Access) Act 1979* once that advice could be given without prejudice to an investigation.

7 Reporting and Oversight

Recommendation 9

That proposed new paragraph 186(1) (ca) of the *Telecommunications (Interception and Access) Act 1979* be amended to require that the Australian Federal Police report to the Minister:

- the number of authorisations for disclosure of telecommunications data to a foreign country;
- identify the specific foreign countries that have received data;
- the number of disclosures made to each of the identified countries; and
- any evidence that disclosed data has been passed on to a third part or parties.

8 Industry Data Handling and Privacy Obligations

Recommendation 10

That the Attorney-General consult initially with the telecommunications industry and then with relevant Ministers, statutory bodies, and public interest groups to clarify and agree on the data handling and protection obligations of carriers and carriage service providers.

Recommendation 11

That the Cybercrime Legislation Amendment Bill 2011 be amended to require carriers and carriage service providers to destroy preserved and stored communications and telecommunications data or a record of that information when that information or record is no longer required for a purpose under the *Telecommunications (Interception and Access) Act 1979* unless it is required for another legitimate business purpose.

Recommendation 12

That the exemption of small Internet Service Providers from the *Privacy Act 1988* as small businesses be reviewed by the Attorney-General with a view to removing the exemption.

9 Industry Implementation Issues

Recommendation 13

That the Attorney-General's Department consult widely with carriers and carriage service providers to ensure that the Cybercrime Legislation Amendment Bill 2011, when enacted, can be implemented in a timely and efficient manner.